General Services Administration
Information Security Oversight Office
Washington, DC 20405

JUN 22 1982

Honorable Glenn English
Chairman
Subcommittee on Government Information
and Individual Rights
Committee on Government Operations
House of Representatives
Washington, DC 20515

Dear Mr. English:

I enclose answers to the 25 additional questions on the executive branch's information security system that you posed for the Subcommittee on Government Information and Individual Rights in your letter to me of May 18, 1982. I have coordinated a number of these answers with officials of other concerned agencies. If an answer includes input from another agency, I have indicated that fact by naming the agency at the conclusion of the answer.

Please let me know if I can be of further assistance to the Subcommittee.

Sincerely,

Steven Garfinkel

STEVEN GARFINKEL
Director

Enclosure

STAT cc: CIA - [redacted]

Added distribution: (D/OIS:ydc/25 Jun 82)
1 - C/RMD
1 - C/IPD
1 - C/CRD

ADDITIONAL QUESTIONS: EXECUTIVE ORDER ON SECURITY CLASSIFICATION

1. The Order defines "national security" in terms of national defense and foreign relations. What does "foreign relations" mean?

   Answer: "Foreign relations" means all matters relating to the formulation, execution and conduct of United States foreign policy, including but not limited to United States relations with foreign governments and international organizations, both at the present time and in the foreseeable future. (Department of State)

2. Are there any decided FOIA cases that would have different results under the new Executive Order? Which ones and why would a different result be indicated?

   Answer: The only case in which the result, now on appeal, might have been different under the new Executive order is Taylor v. Department of the Army, Civil Action No. 81-2353 (D.D.C. November 20, 1981), appeal docketed, No. 81-2280 (D.C. Cir. December 4, 1981). In Taylor the Army classified as Confidential "measured resource area ratings" on the basis that they concerned "military plans, weapons or operations" (section 1-301(a), E.O. 12065), the release of which reasonably could be expected to cause at least identifiable damage to the national security (section 1-104, E.O. 12065). The district court concluded that an Army regulation precluded classification, but went on to find that it was improper to classify substantively the ratings under E.O. 12065. In so doing, the district court questioned whether the ratings revealed military capability and concluded that the government's affidavits failed to establish that release of the ratings reasonably could be expected to cause at least identifiable damage to the national security.

   Executive Order 12356 gives more descriptive categories of materials that are classifiable, which the ratings more clearly come within, and it also lessens the burden of quantifying the harm necessary to establish the appropriateness of classification that has resulted from the "identifiable" standard. Thus, the district court might have concluded that the agency met its burden of establishing classification under Executive Order 12356, which allows information to be considered for classification if it concerns "the vulnerabilities or capabilities of systems, installations, projects or plans" (section 1-3(a)(2)), if disclosure would cause harm to the national security (section 1-6), as opposed to identifiable harm to the national security.

   Also, there are two cases involving section 3-303, the balancing provision, in which the government was ordered to make additional determinations. In Kanter v. Department of State, 479 F. Supp. 921 (D.D.C. 1979), the court ordered the State Department to balance, but ultimately upheld the balancing determination. In Marks v. Casey, Civil Action No. 77-1108 (D.D.C., July 28, 1981), the court ordered the Central Intelligence Agency (CIA) to consider whether balancing was required pursuant to CIA regulations promulgated to implement E.O. 12065. The court has ordered the CIA to submit additional support for its conclusion that balancing is not required in that case. (Department of Justice)

3. Two of the three limitations on classification that appear in the Carter Order were removed. Did the presence of the two deleted limitations cause any problems or misunderstandings for officials with classification authority?

Answer: I presume that the limitations to which the question refers are sections 1-603 and 1-604 of E.O. 12065. To my knowledge these provisions caused no problems or misunderstandings for officials with classification authority. As stated in my testimony, these provisions were deleted because the requirements for classification make them redundant. The limitations on classification referenced in these provisions continue to be in force under E.O. 12356.

4. Why was "cryptology" added as a new classification category? Is sensitive cryptological information classified now? Is there any cryptological information that should be protected that cannot now be classified?

Answer: The appearance of "cryptology" as a classifiable category of information is not new. The classifiability of this type of information was clearly recognized in previous Executive orders, including E.O. 10501 and E.O. 11652. The drafters of E.O. 12065 omitted specific reference to "cryptology" because they believed that it was adequately covered by the other classification categories. However, experience indicated that while the other categories make clear the classifiability of signals intelligence, similar protection for communications security information, the other element of cryptologic information, was not as apparent. The decision was made to clarify this issue by including "cryptology" as a classification category under E.O. 12356. This addition should not result in an increase in the amount of information classified under the new Order since it covers the same type of information that is currently being classified under E.O. 12065. (Department of Defense)

5. Have sanctions ever been imposed on any federal employee for overclassifying information? Is so, please provide details.

Answer: ISOO surveyed the major classifying agencies following the receipt of this question, and to this date has not uncovered any examples.

6. (a) The definition of "information" in the order uses the words "controlled by the government." When is information under the control of the government?

(b) Is information that is subject to export controls considered to be "controlled by the government" within the meaning of this definition? Does the answer depend on the type of license required under federal law for the export of the information?

Answer: As used in E.O. 12356, "control" refers to the executive branch's ability to govern the dissemination of and access to the information in question. "Control" under E.O. 12356 does not pertain to export controls; however, some information subject to export controls may also be classified if it meets the criteria of E.O. 12356, including "control by the government." (Department of State; Department of Defense)

7. In responding to questions about reclassification of information under the new order, you stated that "hopefully the situation will be one of complete volunteerism on the part of the receiver of the information." If a person refuses to give up information for reclassification voluntarily, under what statutes can the government take action to recover the information?

Answer: The executive has the constitutional and statutory responsibility to protect and control access to national security information. Such information is protected by a classification system embodied in Executive Order 12356 and overlaid with various statutory protections and penalties for its unauthorized disclosure. 5 U.S.C. §552(b)(1); 35 U.S.C. §§181-188; 18 U.S.C. §§792-798; 50 U.S.C. §§781-785. This scheme establishes a government monopoly in the creation and use of classified information. Persons without requisite clearance and authority have no right to possess or use classified information that is properly classified pursuant to the Order. This extensive statutory and regulatory framework gives the government a protectable property interest in properly classified information.

The government could proceed under a non-statutory cause of action in the nature of replevin, based upon the sovereign's inherent right to protect its proprietary interests. The government's power to institute litigation to safeguard government property stems from the broad grant of authority given the Attorney General by Congress, 28 U.S.C. §§ 501, 503, 516, 518, and from a long lineage of Supreme Court cases sustaining the inherent power of the government to protect its property interests. See Benten v. Woolsey, 37 U.S. (12 Pet.) 25 (1838) (mortgage foreclosure suit); United States v. Gear, 44 U.S. (3 How.) 120 (1845) (injunction to restrain waste on public land); Cotton v. United States, 52 U.S. (11 How) 241 (1850) (suit for treaspass onto public land); see also Note, Nonstatutory Executive Authority to Bring Suit, 85 Harv. L. Rev. 1566, 1579-81 (1972). The power to bring such suits has been considered a logical and necessary adjunct to the executive's power to oversee the national government's proprietary interests. See also United States v. California, 332 U.S. 19 (1947) (action to protect United States tidelands). A lawsuit commenced pursuant to the sovereign's inherent powers can rely upon state law causes of action as well. Cotton v. United States, supra, 52 U.S. at 224. (Department of Justice)

8. You testified that the new classification category covering "systems, installations, projects, or plans relating to national security" was intended to cover information concerning protection of the President and the embassies and civil preparedness. Was there any other specific type of information that this category was intended to cover?

Answer: These examples are three general, but very important, subject areas about which information must sometimes be classified, and which do not fit neatly within any of the classification categories under E. O. 12065. The new "vulnerabilities and capabilities" category of E. O. 12356 covers them adequately without necessitating separate categories for each. At the same time there may be other general or specific subject areas requiring classification that may fall within this category, e.g., the military preparedness data at issue in Taylor, supra, No. 2. To my knowledge, however, no other general subject areas were involved in formulating the new "vulnerabilities and capabilities" category.

9. During a discussion of the potential for overclassification of information, Mr. Willard responded to a question by asking: "What is the harm of overclassification?" From the perspective of ISOO, could you provide an answer to Mr. Willard's question?

Answer: In speaking of "overclassification" I assume that the question pertains to the issue of classifying information that does not require classification, rather than those instances in which properly classified information is overgraded. Mr. Willard

has indicated to me that his statement was intended to relate to overclassification solely in the context that initial overclassification does not significantly impact on the public disclosure of material inasmuch as documents, whether classified or not, are considered for disclosure to the public upon request by a member of the public. ISOO certainly concurs that the most critical problem concerning overclassification is its impact on public disclosure, and that the problem of overclassification is almost always resolved as a result of public requests for disclosure. ISOO further recognizes that it is in the context of public access demands that the litigators of the Justice Department ordinarily become involved in the classification process.

There are other reasons that ISOO does not condone overclassification, and gives priority to preventing it through its oversight activities. Overclassification results in far greater costs to the government and taxpayer to create, store, transmit, maintain and destroy information. It also lessens intra-agency or inter-agency accessibility, which may impact adversely on the decision-making process. (These problems are also a product of overgrading, but to a lesser extent.) Finally, and most importantly save for public access, a pattern of overclassification tends to subvert the entire information security system, jeopardizing the respect necessary to protect information that truly warrants classification. (Department of Justice)

10. (a) In your discussion of the new classification category for confidential sources, you stated that some agencies have severe problems with the idea of identifying some of its sources as intelligence sources. How do the sources know on what basis their identity is classified? Have agencies reported actual complaints to your office?

(b) You also indicated that classification of some sources as confidential sources creates problems with an agency's relationship with these sources. What type of problems were reported to your office?

Answer: The Department of State has reported to ISOO the following scenario in which a source may determine the manner in which his or her identity is being protected. There may be a press briefing in which the Department of State releases certain information and indicates that the information was received from a "confidential" source, rather than an "intelligence" source. The source can recognize himself or herself from the information released and reported in the press. Usually, the source does not want to be identified, even indirectly, as an "intelligence" source, a label that may cause uneasiness or worse in some parts of the world. Even though the likelihood of his or her name surfacing is remote, it is still deemed preferable to be identified as a "confidential" source.

The Department of State has also reported that it is concerned lest a court consider that sources of, for example, clearly political or economic information are not, in fact, intelligence sources within the generally accepted meaning of the term, and that they cannot therefore, be validly protected under the category "intelligence sources and methods." Specific provision is required to protect these non-intelligence sources of information. (Department of State)

11. (a) Please provide for the record an estimate of the number of documents that are classified each year throughout government.

(b) Please provide for the record an estimate of the number of documents that are declassified each year.

(c) Please provide for the record a rough estimate of the total number of classified documents that now exist in government files.

(d) Please provide for the record a list of all FOIA cases decided in the last five years in which classified documents were reviewed by the court and the number of classified documents that were reviewed in each case.

Answer:

(a) ISOO estimates that between 800,000 and 1 million documents, depending upon world events, are classified originally each year. Approximately, another 16,000,000 documents are classified derivatively.

(b) Declassification estimates are available by page count, not documents. ISOO estimates that approximately 20 million pages of classified information are declassified annually. (GSA - National Archives and Records Service)

(c) The only rough estimate available is for the number of pages of classified records and presidential papers of permanent historical value located in the repositories of the National Archives. These total approximately 621 million pages. It would take many months and presently unavailable resources to estimate the total number of classified documents worldwide. (GSA - National Archives and Records Service)

(d) Numerous submissions of classified documents in camera have been made in Freedom of Information Act (FOIA) cases in the last five years. The number of classified documents submitted varies according to the scope of the FOIA request. As a rough estimate of the number of FOIA cases involving the withholding of classified materials, the latest edition of the Freedom of Information Case List (September, 1981) lists over 100 FOIA cases involving Exemption 1, the exemption which permits the withholding of classified material. Since the FOIA permits in camera review of all material withheld, in camera review would be possible in every FOIA case involving classified material. Indeed, the Court of Appeals for the D.C. Circuit has found that in camera inspection is often necessary in Exemption 1 cases. See Allen v. Central Intelligence Agency, 636 F.2d 1287, 1298 (D.C. Cir. 1980). A more specific answer to this question cannot be provided without an examination of individual case files, which are scattered in courthouses and records repositories around the United States. This would require substantial resources that are not presently available. (Department of Justice)

12. Who decided that the Carter Order needed to be revised and on what basis? When was the decision made? Were agencies asked for their views at this stage?

Answer: Technically, only the President could make the actual decision to revise E. O. 12065, and President Reagan made it when he signed E. O. 12356 on April 2, 1982. Of course, the President acted only after many months of consideration of prospective revisions by his White House aides, officials of many executive branch agencies, selected Committees of Congress, and representatives of non-governmental groups interested in the information security system. To my knowledge, the first official call for revision to E. O. 12065 occurred during the last year of the Carter Administration. The Comptroller General issued a report on October 15, 1980, calling for the amendment of E. O. 12065 for the purpose of

abolishing the systematic review for declassification program. Prior to the issuance of the final Report that included this recommendation, the GAO had circulated a draft to ISOO for comment in the late Spring, 1980. On June 20, 1980, I convened a meeting of the Interagency Information Security Committee to consider the executive branch's response to the draft Report. At that meeting, representatives of the major classifying and declassifying agencies discussed possible revisions to the systematic review system, as well as other aspects of E. O. 12065. Following that meeting, I initiated ISOO studies of several areas of concern in the Order. ISOO continued to receive informal agency complaints about different sections of E. O. 12065 in the ensuing months. In February 1981, I convened another meeting of the interagency committee, and followed that meeting by calling for specific agency recommendations for amendments to E. O. 12065. This request came simultaneously, but independently, of White House Counselor Edwin Meese's request to the agencies of the intelligence community for prospective amendments to E. O. 12036 and E. O. 12065 that would enhance the United States' intelligence capabilities. These efforts with respect to E. O. 12065 were subsequently merged under ISOO's aegis.

13. Once the decision to modify the Carter Order was made, were agencies asked for their suggestions prior to the circulation of a draft order? Is so, when? Which agencies were asked and which responded to the request?

Answer: Following the February 11th meeting of the Interagency Information Security Committee (see No. 12, above), I sent a letter to the agencies represented on the Committee (State, Treasury, Justice, Defense, Energy, CIA and GSA/Archives) requesting their suggestions concerning prospective amendments to E. O. 12065. I requested responses by March 23, 1981, and received these responses from each of these agencies except the CIA and Treasury.

In the meantime, an intelligence community task force chaired by the CIA had been established to respond to Mr. Meese's request (see No. 12, above). The task force consisted of representatives from many of the same agencies on the Interagency Committee. The task force determined to draft a rewrite of E. O. 12065, rather than merely submit proposed amendments. It submitted a draft to Richard Allen, Assistant to the President for National Security Affairs, on August 28, 1981. On September 2, 1981, Mr. Allen submitted this draft to me with instruction to coordinate further with executive branch agencies in the development of a replacement to E. O. 12065.

14. How many drafts were prepared and formally circulated to agencies prior to submission of the final draft to the President? When was each draft circulated and how long were agencies given to comment?

Answer: The intelligence community task force draft served as a framework for ISOO in its development of a draft Order to be circulated for further agency comment. ISOO revised the intelligence community draft based upon the suggestions it had received in response to its own previous request, and ISOO's oversight experience with E. O. 12065, including its studies of certain aspects of the Order. ISOO circulated its first draft to 33 executive branch agencies or offices within the Executive Office of the President on October 16, 1981.

Agencies were given 30 days to reply, although several of the eventual responses arrived somewhat later. Based upon these comments, ISOO submitted a revised draft to the Acting Assistant to the President for National Security Affairs on December 4, 1981. The Office of Management and Budget forwarded it to the Office of the Vice President and ten of the major classifying agencies for comment on December 23, 1981. Agencies were asked to submit comments on this version by January 18, 1982. All agencies submitted comments. ISOO prepared a third draft dated February 2, 1982. During February 1982, the ISOO briefed congressional committees and private interest groups on the proposed Order and requested any comments they might wish to make. Most submitted oral or written recommendations for change.

The comments received were incorporated into the fourth ISOO draft, which was submitted to the Assistant to the President for National Security Affairs on March 8, 1982. Following some coordination between the ISOO and the Executive Office of the President, the Order was signed by the President on April 2, 1982.

15. Did the Administration ever make a formal public announcement that a revision of the security classification order was either being considered or was underway? If so, who made the announcement and when? Please provide a copy for the record.

Answer: No.

16. In your testimony, you listed a number of groups that you consulted during the revision process. Is that list complete? If not, please complete the list.

Answer: The list is complete.

17. Were any of these groups provided a copy of a draft order or permitted to review a copy? If so, for each group, list the dates when copies were provided or when review was permitted.

Answer: Each group had an opportunity to review a copy of the draft Order. The pertinent dates are as follows:

The American Bar Association Task Force on Government Information and National Security ——— February 11, 1982

The American Council on Education ——— Feburary 5, 1982

The American Historical Association ——— February 23, 1982

The Association of Former Intelligence Officers ——— February 16, 1982

The Center for National Security Studies ——— February 10, 1982

The Institute of Electrical and Electronics Engineers ——— February 18, 1982

The National Classification Management Society ——— February 10, 1982

18. How were the comments or suggestions of these groups used in preparing the final order?

The comments and suggestions of these groups were considered along with those of the agencies in revising and preparing the final draft of the Order. For example, the concern expressed by some of the groups over basic scientific research data resulted in the explicit restoration of the prohibition against classifying basic scientific research not clearly related to the national security. Other concerns expressed by the groups relating to possible abuse resulted in strengthening or adding oversight controls for the Information Security Oversight Office. In addition, the ISOO implementing directive will reflect a number of comments received from these interest groups or the congressional committees.

19. Were there any groups that expressed interest in the Executive Order that were not offered an opportunity for a formal consultation?

Answer: No.

20. Were there any groups that your office consulted with about the Executive Order revisions that had not first contacted you to express interest in the revision process?

Answer: Yes. ISOO contacted two of the groups entirely on its own initiative in the belief that they represented interested parties that were not otherwise represented by the other groups with which ISOO was consulting. These were the American Historical Association and the Association of Former Intelligence Officers. ISOO also initiated contact with two of the other groups following notification to ISOO by third parties that these groups were interested in the proposed Order. These were the American Council on Education and the American Bar Association Task Force on Government Information and National Security.

21. Were any of the drafts ever released for public comment by the Reagan Administration? If not, why not?

Answer: No, if the question refers to general public comment. By soliciting comment from interested congressional committees and non-government interest groups representing a spectrum of opinion, the Administration took extraordinary steps to seek a wide range of comment in an exercise that is ordinarily closed to anyone outside the executive branch. The scope of comments received and considered certainly reflects the broad degree of input solicited from outside the executive branch.

22. The Carter Administration released draft Executive Order on Security Classification for public comment. At what stage in the revision process was the draft order released?

Answer: The significant difference between the process for outside comment between E. O. 12065 and E. O. 12356 only appears to have been in timing; i.e., the first formal draft of E. O. 12065 was circulated to groups that had expressed an interest in the proposed Order. Early in the development process for E. O. 12065,

two individuals and several private interest groups made it known to the Carter Administration that they had an interest in the plans to change the Executive order on national security information. On September 13, 1977, copies of the proposed draft were made available to those individuals and groups by representatives of the Domestic Policy Staff and the National Security Council. This was the first of three drafts of the order and the only that appears to have been circulated for comment outside the executive branch.

23. How was the Carter draft order circulated? How long was allowed for public comments? How many comments were received and who submitted the comments?

Answer: In addition to the circulation process described in No. 22, above, the Office of Management and Budget circulated the draft of the order to the agencies for comment. Individuals and private interest groups provided access to the draft order were asked to provide comments within 30 days. Comments were received from the following:

National Classification Management Society
Mr. Robert Singel
Mr. William Florence

A combined response representing the views of:

American Civil Liberties Union
Project on National Security and Civil Liberties
Center for National Security Studies
National Committee Against Repressive Legislation Common Cause
Public Citizen Litigation Group
Committee for Public Justice
American Ethical Union.

In addition, comments were received from the following congressional committees:

Subcommittee on Intergovernmental Relations of the Senate Committee on Governmental Affairs

Subcommittee on Government Information and Individual Rights of the House Committee on Government Operations.

24. Early this year, press accounts indicated that a multi-volume set of intelligence documents taken from the American embassy in Teheran was being sold openly. Some of the documents reproduced in these books reportedly were pieced together from shredded copies. What new document destruction techniques are available to preclude reconstruction of classified information that has been supposedly destroyed?

Answer: The suggested responses to this question, as presented to ISOO by the Department of State, Department of Defense and Central Intelligence Agency, respectively, are reproduced verbatim as Appendix A to these answers.

25. What kinds of emergency planning regarding the protection, removal, or destruction of classified material have been developed to avoid the loss of classified information such as occurred in Saigon and Teheran?

Answer: The suggested responses to this question, as presented to ISOO by the Department of State, Department of Defense and Central Intelligence Agency, respectively, are reproduced verbatim as Appendix B to these answers.

APPENDIX A

Department of State

24. The Office of Security has approved a number of different types of destruction equipment that, when properly operated, definitely prevent any meaningful reconstruction of paper documents. Approved equipment of this type is referred to as terminal destruction equipment and includes several cross-cut shredders. Terminal destruction equipment is normally afforded backup generator power designated for the use of selected equipment during power failures and/or other emergency situations.

Other shredders are also approved for the use in Department of State facilities, but not for terminal destruction. These shredders are known as "strip shredders" which simply slice paper into narrow strips. Classified material that has been sliced into strips is still handled as classified material until it is finally destroyed by an approved method.

There is some belief that it was one of these strip shredders that was hastily and improperly utilized during the November 4, 1979, Tehran incident that contributed to the loss and compromise of some classified material.

The Department continues to encourage all overseas posts to reduce and maintain total classified holdings at the minimal level consistent with sound emergency planning.

Department of Defense

"Many of the methods of destruction in use and which have been in use for a long time preclude reconstruction of classified information which has been destroyed. Examples of these methods are burning, melting, chemical decomposition, pulping, pulverizing, or mutilation sufficient to preclude recognition or reconstruction of the classified information. The problem exists in that these methods generally require time and many can be interruped before destruction is complete. Accordingly, the Department of Defense has established a requirement for anticompromise emergency destruction (ACED). Very simply, this requirement provides that, if highly classified material cannot be afforded protection from hostile elements in an emergency situation, then provision shall be made for the installation of suitable ACED systems. An ACED system is one that shall reach a stage in destruction sequences at which positive destruction is irreversible within 60 minutes at shore installations, 30 minutes in ships, and 3 minutes in aircraft following activation of ACED systems. In accordance with existing directives, the Navy is responsible for and is developing ACED systems. Acceptance by the Military Services is expected by the beginning of the second quarter of FY 1983 with equipment delivery beginning in the first quarter of FY 1984. Information concerning ACED systems may be made available to non-DoD departments and agencies."

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200010005-3

Next 3 Page(s) In Document Exempt

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200010005-3

APPENDIX B

Department of State

25. The following information is presented re the Protection of Post Information Procedures that have been instituted since SAIGON:

1. A Microfiche Program has been designed to afford reconstitution of files, drastically reduce destruction time by eliminating paper files, and provide more time for personnel to attain safety of a secure area should the situation arise.

2. Readers have been provided the thirty-eight (38) posts that are participating in this microfiche program.

3. Participating posts have been issued Microfiche Destruction Kits which are used with this system. These microfiche records can be destroyed in two (2) minutes using the specially provided chemical solution.

4. Accelerated retirement of records has been recommended for threat posts. This action results in only 1981 and 1982 subject records being kept at post, i.e., current and previous year.

5. Duplicate files, drafts and obsolete material are to be eliminated. Instructions have been provided to posts and briefings are given to all CPO's* going to post.

6. Emergency and Evacuation Plans are reviewed by Security officers, Foreign Service Inspectors and Security Enhancement Survey Teams. Particular attention is paid by Foreign Affairs Information Management (FAIM) to their practical aspects, namely capability of enhancing preservation of life by destruction of classified and unclassified/sensitive information.

7. The safehavening of sensitive records is encouraged and FAIM serves as point of safehaven.

8. The distribution of classified cables is to be limited to Embassy personnel who have a requirement to know and respond.

9. Destruction of unneeded classified material is to be done on a daily basis.

Department of Defense

"Immediately following the incident in Iran, the Department of Defense initiated an in-depth review of the circumstances of the incident for the purpose of evaluating the effectiveness of policies and procedures then in existence for the safeguarding of U.S. classified information stored with DoD activities at overseas locations. As a result of that review, the following additional safegaurding measures were developed and implemented:

- "A requirement that classified information stored in countries other than NATO countries, Australia, New Zealand, or Japan, be maintained under U.S. control on a 24 hour basis.

- "A requirement that all DoD activities develop emergency plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action.

"Such plans are to provide, as a minimum, for:

- "Initial and periodic review of classified holdings to ensure that only the minimum amount of classified information is retained consistent with operational requirements.

- "Establishment of a system of priorities to ensure that classified information is destroyed in the order of its level of sensitivity.

- "Designation of personnel who shall be responsible for accomplishing destruction.

- "Designation of places and methods of destruction.

- "Identification of the individual who is authorized to make the final determination as to when emergency destruction is to begin and the means by which this determination will be communicated to the individual who will be responsible for accomplishing destruction.

- "A requirement for installation of ACED equipment in those special circumstances where normal protection measures cannot be applied (e.g., classified information stored aboard ships or aircraft)."

Next 1 Page(s) In Document Exempt

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200010005-3

TRANSMITTAL SLIP	DATE 28 June 82
TO: C/CRD SK	
ROOM NO.	BUILDING

REMARKS:

OPS

ADMIN

INTEL

S+T

Barb - file w EO 12356

FROM:		
ROOM NO.	BUILDING	EXTENSION

FORM NO. 1 FEB 55 241 REPLACES FORM 36-8 WHICH MAY BE USED. (47)

shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

1.3 (c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

SEC 1.4 Duration of Classification.

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.